Global Cyber Bi-Weekly Report by INSS September 01 2018

Editor-in-chief: Gabi Siboni, **Editor:** Hadas Klein, Gal Perl Finkel

Contributors: Simon Tsipis, Anna Danilova, David Libin, Gal Sapir, Michal Beit Halachmi

ISRAEL

Israeli cybersecurity company Indegy raises $18 million

Indegy, an Israeli cybersecurity firm, has raised $18 million in a financing round led by Liberty Technology Fund, which included an investment by UK energy company Centrica Innovations. Indegy specializes in technology that gives businesses visibility and control over their industrial control systems to protect against cyber threats, malicious insiders, and human error. Totally non-intrusive, the Indegy solution can be deployed with no impact on customers' operations and has been designed to detect anomalies on industrial control systems, using advanced machine-learning technology to analyze and alert users to suspicious activity on their network. Previous investors Vertex Ventures, Aspect Ventures, Magma Venture Partners, and angel investor Shlomo Kramer also participated. The company has raised $36 million total, including the latest financing round. The firm was founded in 2014 by Barak Perelman, Mille Gandelsman and Ido Trivizki, who are graduates of the IDF's Talpiot program.

https://goo.gl/CDGaiS

Exclusive: Ex-Israeli cyber chief sheds light on virtual offensives

The new US Cyber Command head Gen. Paul Naksone said that one main mistake that people make with cyber defense and deterrence is trying to divide everything into peacetime and wartime. He advised avoiding these binary choices and to be prepared for constant low-grade cyber combat. Buky

Carmeli, former director of the National Cyber Security Authority, has said in an interview that he identifies "a lot with what he [Gen. Naksone] says . . . People use lots of physical-world words. You have peacetime, a war like 2014 Operation Protective Edge, a terrorist incident or some other uptick in violence. War in cyber does not have any of this. Cyber is an endless battle—you are always playing chess with the other side." Carmeli, who served twenty-one years in IDF Unit 8200, "the Israeli NSA," and the Defense Ministry, came back to the chess analogy to explain another important point about how countries, including Israel, and private companies should construct their cyber strategies today. "In chess, sometimes you lose a pawn. Maybe you weigh trading losing a bishop in order to take someone else's knight. You need to look at the full spectrum of priorities. And you do not deal with every threat," he said.

https://goo.gl/yLSvcc

UNITED STATES

PG&E, an energy company, agreed to 2.7 million settlement for breaking cybersecurity regulations

PG&E had left 30,000 records online for seventy days in 2016. This information contained usernames and passwords, which could enable access to sensitive information. The settlement agreement was reached over two violations of the Critical Infrastructure Protection NERC Reliability Standards with the Western Electricity Coordinating Council, a body tasked with making companies comply with federal standards in the western United States. PG&E's IT team seems to have covered up the exposed files, by saying that the data was not critical. However, the settlement indicates otherwise.

https://bit.ly/2wv11GI

T-Mobile data breach exposes 2.3 million customers, and hacker seems to want to sell the data

The data of 2.3 million T-Mobile customers has been exposed, and the hacker seems to want to sell the data. T-Mobile released a statement in which it indicated that no credit card numbers, passcodes, or social security numbers had been exposed. The statement was later revised to include the exposure of encrypted passwords. The hack was conducted via a vulnerable application programming interface. The fact that T-Mobile data was leaked via MDF, which is considered easier to randomly generate passwords, indicates that the company is not keeping up with the best cybersecurity standards.
https://bit.ly/2NmH6kx

Instagram says users can now evaluate authenticity of accounts

Similar to parent company Facebook, Instagram has launched "About This Account" feature, allowing its more than one billion users to evaluate an account running advertisements, geographic location, and username changes among other elements. The social media platform will allow third-party apps, such as DUO Mobile and Google Authenticator, for two-factor authentication, increasing the layer of security. Initially, this feature will extend to users managing pages with a significant US following and will continue to extend in availability.
https://reut.rs/2NtuUyp

Facebook shuts 652 Iran-backed accounts linked in global disinformation campaign

The cybersecurity firm FireEye has uncovered a network of accounts, some active since 2013, that have been engaged in a coordinated influence campaign. The spread of political disinformation in an effort to manipulate political discourse targeted a magnitude of international users. Another part of the network dating back to 2016 was discovered to have initiated malware

attacks though account breaches. In response to the alert, Facebook, followed by Twitter, collectively removed over 900 accounts, pages, and groups. According to the company, the fake accounts posed as news and civil society organizations published content in multiple languages; articulating anti-Saudi, anti-Israeli, pro-Palestinian, and US policies favorable to Iran. The common thread of the shared content originates from "Liberty Front Press," a site linked to an Iranian state media outlet. Facebook discovered accounts involved in disinformation efforts linked to a Russian military intelligence unit, unassociated with the Iranian campaign, sheds light on the news that was revealed the same day by Microsoft. Microsoft had revealed ahead of the November congressional elections that the Russian-backed group called Fancy Bear or APT28 attempted a phishing operation targeting conservative American think tanks and the US Senate, and consequentially over eighty counterfeit websites were shut down.
https://n.pr/2BOiyj9

Google removes YouTube channels and web accounts tied to Iran

Following the actions of Facebook and Twitter, with the assistance of cybersecurity firm FireEye, Google also identified and removed over fifty channels and webpages associated with Iran Broadcasting, a state-run media outlet. Since the 2016 election interference and the upcoming November midterm elections, technology companies are in the spotlight in policing and preventing state-sponsored hacking and manipulation of services resulting in influence campaigns. Executives from Google, along with other social media companies, are scheduled to testify before a Senate Intelligence Committee hearing regarding foreign election interference on September 5.
https://bloom.bg/2Pdg4wk

EUROPE

EU considers 60-minute deadline for social networks to remove terrorist content

The European Commission is considering imposing an hour-long deadline for social networks to remove terrorist and extremist content after voluntary measures appear to have failed. As reported by the Financial Times, Facebook, Twitter, and YouTube, as well as smaller businesses, are all within the European Commission's sights. This is the first time that technology firms and online services could be held directly responsible for how long terrorism-related content is allowed to circulate on social media.
https://zd.net/2N4S5Pk

Europe worries as Facebook fights manipulation worldwide

Europe—where Facebook has more users than in the United States—is particularly worried that the region will become a regular target of foreign propaganda efforts, including ahead of next year's European Parliament elections, which will help set the policy direction in Brussels for the next five years.
https://nyti.ms/2P0VpM0

British fear the AI future as 60 percent are worried AI machines will hack them

New research from IP EXPO Europe uncovers the concerns the general public has about artificial intelligence (AI) and cybersecurity. With AI assistants as part of our daily lives, new research from IP EXPO Europe—Europe's number one enterprise IT event—has found 60 percent of the British are worried that artificial intelligence (AI) will hack their internet connected devices. The research, which studied the perception that the UK public has toward AI used in both cybersecurity and cyberattacks, also found just over a quarter believe cyber criminals are not capable of using AI, claiming it is too expensive, too complicated to use, and simply not having access to it.

https://bit.ly/2oktKKx

Cybersecurity staff shortage leads to services spend

Security spending globally is forecast to rise by almost a quarter to hit $124.12 billion in 2019, largely driven by the low supply of highly skilled talent and regulatory changes. That figure is according to Garner analysts, who predict that this year alone security spend is set to rise 12 percent from $101.54 billion to $114.15 billion. Siddharth Deshpande, research director at Gartner, said, "Persistent skills shortages and regulatory changes like the GDPR in Europe are driving continued growth in the security services market."
https://bit.ly/2PMcWZv

Bank of Spain hit by DDoS attack causing its website to be intermittently offline

Banco de España says the DDoS disruption did not have any effect on the organization's operations. It said communications with the European Central Bank were unaffected and that there was no evidence that it had suffered any type of data breach. "We suffered a denial of service attack that intermittently affected access to our website, but it had no effect on the normal functioning of the entity," a spokesperson told the Information Security Media Group. "As we are the national central bank of Spain, not a commercial bank, we offer no banking services—on-site or online—to individuals nor firms."
https://bit.ly/2wveXQT

Germany, seeking independence from United States, pushes cybersecurity research

Germany announced a new agency to fund cutting-edge research on cybersecurity and to end its reliance on digital technologies from the United States, China and other countries. Interior Minister Horst Seehofer told reporters that Germany needed new tools to become a key player in the field

of cybersecurity and shore up European security and independence. The agency is a joint interior and defense ministry project.
https://bit.ly/2POtfEX

RUSSIA

Russian hacker might posses the link to Russian involvement in US election fraud

As was reported by the news agency Bloomberg, in reference to sources in the US Department of Justice, US investigators are trying to find out what information about the alleged interference of Russia in the US election the Russian hacker Evgeny Nikulin has. According to law enforcement officials, the hacker is accused of hacking the LinkedIn social network and may have important information regarding the US election fraud and the link to Russian involvement.
http://bit.ly/2Ns2tB1

Telegram agreed to provide the Russian Security Services with encryption keys

The Telegram messaging social network, which was under unprecedented pressure from the Russian Security Services to deliver encryption keys to the service in order to decode its clients' correspondence, published on its official website an updated privacy policy. The policy states that the messenger's administration undertakes to provide law enforcement with information about users suspected of terrorist activity and if there is an appropriate request from a court. In addition, every six months Telegram will publish reports on its cooperation with special services against terrorism.
http://bit.ly/2BVzoMP

Russian military launched special mobile teams for combating drones

On the basis of its Syrian experience, units for combating UAVs have been formed in the units of the Southern Military District, the Russian Ministry of Defense reported. Earlier similar forces appeared in the Western and Central Military Districts, in Kyrgyzstan and Tajikistan Russian Army bases. According to the report, the units of the REB (electronic warfare) will fulfill the tasks of suppressing radio communications in various ranges, inflicting radio-electronic strikes on control points and communication centers of the enemy, including control and data transmission channels for small-size unmanned aerial vehicles.
http://bit.ly/2wuLyq3

New radio-electronic weaponry from Kalashnikov

Russian Military and other Security and Law enforcement agencies soon to receive a newly developed radio-electronic non-lethal weaponry from "Kalashnikov" concern. The first REX-1 radio-electronic gun from "Kalashnikov" is designed to suppress and disable unmanned aircrafts (UAV's).
http://bit.ly/2MxFvMh

MIDDLE EAST

According to recent statistics, 48 percent of cyberattacks in the Middle East result in the theft of more than $500,000.

Only 43 percent of companies have an adequate level of protection against attacks, according to a report by Kaspersky labs. Some 58 percent of businesses had to manage an outage of more than five hours. The UAE was subjected to a high number of the Middle East attacks due to its high use of password-only authentication. More than half the UAE adult population has been a victim of cybercrime in 2017. The growing importance of cybersecurity will affect the profitability of Middle Eastern firms if they do not secure their

systems, according to Samina Rizwan, senior director of business analytics and big data for the Middle East Africa at Oracle.
https://bit.ly/2P4yuzg

Trend Micro to set up academy for cybersecurity exclusive to Saudi nationals

Trend Micro, a Japanese cybersecurity and IT company, unveiled an initiative to modernize and enhance Saudi cybersecurity. The initiative will address the shortage of trained cybersecurity expertise in Saudi Arabia. The two-year program will enable graduates in computer science to interact with Trend Micro executives and learn from their experience. Trend Micro has already unveiled this program in Canada, the United States, and Brazil. The initiative is part of the growing push to digitize Saudi Arabia's economy.
https://bit.ly/2P9ywpM

Iranian cyberattacks increasingly targeting for monetary benefits

A report from Eurasia Review shows that many recent cyberattacks from Iran have financial motives. This means that Iran, like states such as North Korea which are shut out of the global financial system, are relying on cyber capabilities to fulfill finance goals. Five ransomware variants were developed or repurposed in Iran, such as Rastakhiz, Tyrant, WannaSmile, Black Ruby, and Android ransomware as identified by Accenture Security's iDefense threat intelligence team. The cyber criminals seem to be cooperating with the Islamic Revolutionary Guard Corps to develop increased cyber capabilities.
https://bit.ly/2ogO3si

LATIN AMERICA

US Secretary of Defense in Chile signs cooperation agreement with Chilean partners, including cybersecurity

The president of Chile expressed his desire to maintain his privileged partnership with the United States and added his interest in cyber cooperation. "A topic that is of great interest is cybersecurity, that is something for which Latin American countries are not well prepared, and we must recover lost time," said President Piñera of Chile. The agreement containing cyber provisions was signed in Santiago, with the defense minister of Chile, Alberto Espina Otero. He said, "the United States has the technology and knowledge, and for us, as a country, it is very important to have with them concrete agreements to carry out training exercises and exchange of information."

https://bit.ly/2MSHQgP

Kaspersky Labs detected malware Dark Tequila used to hack into Mexican banks customers

According to the researchers who detected the malware, Dark Tequila has been operating since 2013, collecting information on customers of banks. Dark Tequila is a multistage malware that spreads through spear-phishing messages and infected USB devices. The Dark Tequila steals financial data from a long list of online banking sites, gathers credentials from popular websites, business and personal email addresses, domain registers, and file storage accounts. Kaspersky Labs indicated that the level of the sophistication was unusual, as it had means of evading detection, and it is able to operate only under certain technical conditions.

https://bit.ly/2POgfiC